WHAT IS CLAIMED IS:

1   1. A method comprising:

2   encrypting a plurality of non-volatile storage
3   regions, each being encrypted using a different
4   encryption key from a set of encryption keys;

5   making a first subset of the encryption keys available
6   to a first user thereby granting the first user access
7   to a corresponding first subset of non-volatile
8   storage regions, the first subset of the encryption
9   keys consisting of one, a plurality, or all of the
10   encryption keys; and

11   making a second subset of the encryption keys
12   available to a second user thereby granting the second
13   user access to a corresponding second subset of non-
14   volatile storage regions, the second subset consisting
15   of one, a plurality, or all of the encryption keys.

1   2. The method of Claim 1, further comprising:

2   generating a first private-public encryption key pair
3   and a second private-public encryption key pair;

4   making the first private key available only to the
5   first user and the second private key only to the
6   second user; and

7   encrypting the first subset of the encryption keys
8   using the first public encryption key, and the second
9   subset of the encryption keys using the second public
10   encryption key.

1   3. The method of Claim 2, further comprising:

2　　　　storing the first private key and the second private

3　　　　key in a secure memory unit;

4　　　　protecting access to the first private key with a

5　　　　first authentication token, the first authentication

6　　　　token being known only to the first user; and

7　　　　protecting access to the second private key with a

8　　　　second authentication token, the second authentication

9　　　　token being known only to the second user.

1　　4. The method of Claim 3, further comprising:

2　　　　requesting an authentication token from a user

3　　　　attempting to access one or more of the non-volatile

4　　　　storage regions;

5　　　　authenticating the user, if the user's authentication

6　　　　token matches one of the authentication tokens used to

7　　　　protect access to one of the private keys;

8　　　　decrypting, with the secure encryption module using

9　　　　the authenticated user's private key, a corresponding

10　　　　subset of encryption keys, in response to

11　　　　authenticating the user; and

12　　　　decrypting a corresponding subset of non-volatile

13　　　　storage regions, thereby making the corresponding

14　　　　subset of non-volatile storage regions available to

15　　　　the authenticated user.

1　　5. The method of Claim 3, wherein the authentication tokens

2　　　　are selected from the group consisting of: passwords,

3　　　　fingerprints signatures, voice signatures, retina

4　　　　signatures, and secure access devices.

1   6. The method of Claim 4, wherein the encrypting and
2   decrypting the plurality of non-volatile storage regions
3   are performed using full-disk encryption software.

1   7. The method of Claim 1, wherein one of the non-volatile
2   storage regions is adapted to store an operating system
3   and data common to the first user and to the second user.

1   8. The method of Claim 1, wherein one of the non-volatile
2   storage regions is adapted to store user-specific data of
3   the first user.

1   9. The method of Claim 1, wherein one of the non-volatile
2   storage regions is adapted to store user-specific data of
3   the second user.

1   10. The method of Claim 1, wherein the non-volatile storage
2   regions are chosen from the group consisting of: volumes,
3   disks, partitions, and folders/directories.

1   11. An apparatus comprising:

2   one or more processors;

3   a memory accessible by the one or more processors;

4   a plurality of non-volatile storage regions accessible
5   by the one or more processors;

6   an encryption unit adapted to encrypt the plurality of
7   non-volatile storage regions, each with a different
8   encryption key selected from a set of encryption keys;

9   wherein a first subset of the encryption keys is
10   made available to a first user thereby granting the

11   first user access to a corresponding first subset of

12   non-volatile storage regions, the first subset of

13   the encryption keys consisting of one, a plurality,

14   or all of the encryption keys; and

15   wherein a second subset of the encryption keys is

16   made available to a second user thereby granting the

17   second user access to a corresponding second subset

18   of non-volatile storage regions, the second subset

19   consisting of one, a plurality, or all of the

20   encryption keys.

1   12. The apparatus of Claim 11, further comprising a secure

2   encryption module adapted to:

3   generate a first private-public encryption key pair

4   and a second private-public encryption key pair;

5   make the first private key available only to the first

6   user and the second private key only to the second

7   user; and

8   encrypt the first subset of the encryption keys using

9   the first public encryption key, and the second subset

10   of the encryption keys using the second public

11   encryption key.

1   13. The apparatus of Claim 12, wherein the secure encryption

2   module is further adapted to:

3   store the first private key and the second private

4   key;

5   protect access to the first private key with a first

6   authentication token, the first authentication token

7   being known only to the first user; and

8   protect access to the second private key with a second

9   authentication token, the second authentication token

10   being known only to the second user.

1   14. The apparatus of Claim 13,

2   wherein the secure encryption module is further

3   adapted to:

4   request an authentication token from a user

5   attempting to access one or more of the non-volatile

6   storage regions,

7   authenticate the user, if the user's authentication

8   token matches one of the authentication tokens used

9   to protect access to one of the private keys, and

10   decrypt, using the authenticated user's private key,

11   a corresponding subset of encryption keys, in

12   response to authenticating the user, and

13   wherein the encryption unit is further adapted to

14   decrypt a corresponding subset of non-volatile storage

15   regions, thereby making the corresponding subset of

16   non-volatile storage regions available to the

17   authenticated user.

1   15. The apparatus of Claim 13, wherein the authentication

2   tokens are selected from the group consisting of:

3   passwords, fingerprints signatures, voice signatures,

4   retina signatures, and secure access devices.

1   16. The apparatus of Claim 14, wherein the encryption unit

2   comprises full-disk encryption software.

1   17. The apparatus of Claim 11, wherein one of the non-
2   volatile storage regions is adapted to store an operating
3   system and data common to the first user and to the
4   second user.

1   18. The apparatus of Claim 11, wherein one of the non-
2   volatile storage regions is adapted to store user-
3   specific data of the first user.

1   19. The apparatus of Claim 11, wherein one of the non-
2   volatile storage regions is adapted to store user-
3   specific data of the second user.

1   20. The apparatus of Claim 11, wherein the non-volatile
2   storage regions are chosen from the group consisting of:
3   volumes, disks, partitions, and folders/directories.

1   21. A computer program product comprising:

2   means for encrypting a plurality of non-volatile
3   storage regions, each non-volatile storage region
4   being encrypted using a different encryption key from
5   a set of encryption keys;

6   means for making a first subset of the encryption keys
7   available to a first user thereby granting the first
8   user access to a corresponding first subset of non-
9   volatile storage regions, the first subset of the
10   encryption keys consisting of one, a plurality, or all
11   of the encryption keys; and

12   means for making a second subset of the encryption
13   keys available to a second user thereby granting the
14   second user access to a corresponding second subset of

15   non-volatile storage regions, the second subset
16   consisting of one, a plurality, or all of the
17   encryption keys.

1   22. The computer program product of Claim 21, further
2   comprising:

3   means for generating a first private-public encryption
4   key pair and a second private-public encryption key
5   pair;

6   means for making the first private key available only
7   to the first user and the second private key only to
8   the second user; and

9   means for encrypting the first subset of the
10   encryption keys using the first public encryption key
11   and the second subset of the encryption keys using the
12   second public encryption key.

1   23. The computer program product of Claim 22, further
2   comprising:

3   means for storing the first private key and the second
4   private key;

5   means for protecting access to the first private key
6   with a first authentication token, the first
7   authentication token being known only to the first
8   user; and

9   means for protecting access to the second private key
10   with a second authentication token, the second
11   authentication token being known only to the second
12   user.

1   24. The computer program product of Claim 23, further

2   comprising:

3   means for requesting an authentication token from a

4   user attempting to access one or more of the non-

5   volatile storage regions;

6   means for authenticating the user, if the user's

7   authentication token matches one of the authentication

8   tokens used to protect access to one of the private

9   keys;

10   means for decrypting, using the authenticated user's

11   private key, a corresponding subset of encryption

12   keys, in response to authenticating the user; and

13   means for decrypting a corresponding subset of non-

14   volatile storage regions, thereby making the

15   corresponding subset of non-volatile storage regions

16   available to the authenticated user.

1   25. The computer program product of Claim 23, wherein the

2   authentication tokens are selected from the group

3   consisting of: passwords, fingerprints signatures, voice

4   signatures, retina signatures, and secure access devices.

1   26. The computer program product of Claim 24, wherein the

2   means for encrypting and the means for decrypting the

3   plurality of non-volatile storage regions comprises full-

4   disk encryption software.

1   27. The computer program product of Claim 21, wherein one of

2   the non-volatile storage regions is adapted to store an

3   operating system and data common to the first user and

4   the second user.

1   28. The computer program product of Claim 21, wherein one of

2   the non-volatile storage regions is adapted to store

3   user-specific data of the first user.

1   29. The computer program product of Claim 21, wherein one of

2   the non-volatile storage regions is adapted to store

3   user-specific data of the second user.

1   30. The computer program product of Claim 21, wherein the

2   non-volatile storage regions are chosen from the group

3   consisting of: volumes, disks, partitions, and

4   folders/directories.

5